BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 769 446**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **97 12277**

(51) Int Cl[6] : H 04 L 9/28, H 04 L 9/32, H 04 Q 7/20, 7/08

(12) DEMANDE DE BREVET D'INVENTION A1

(22) Date de dépôt : 02.10.97.

(30) Priorité :

(43) Date de mise à la disposition du public de la demande : 09.04.99 Bulletin 99/14.

(56) Liste des documents cités dans le rapport de recherche préliminaire : *Se reporter à la fin du présent fascicule*

(60) Références à d'autres documents nationaux apparentés :

(71) Demandeur(s) : *DELAHAYE ACHILLE JOSEPH MARIE FRANCOIS* — FR.

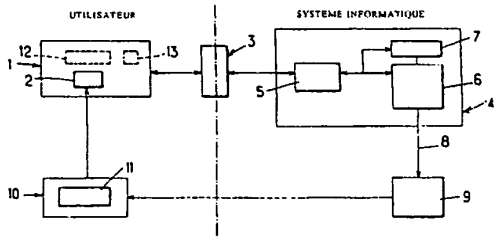
(72) Inventeur(s) : DELAHAYE ACHILLE JOSEPH MARIE FRANCOIS.

(73) Titulaire(s) :

(74) Mandataire(s) : CABINET DE BOISSE.

(54) SYSTEME D'IDENTIFICATION ET D'AUTHENTIFICATION.

(57) Ce système d'identification et d'authentification vis-à-vis d'au moins une unité électronique comprend des moyens d'interface (1, 3) pour l'introduction de données d'identification et/ ou d'authentification, des moyens 5, 6, 7) d'identification d'utilisateurs, des moyens (5, 6, 7) pour générer un code variable en réponse à l'identification d'un utilisateur, des moyens (9, 10) pour transmettre ledit code variable audit utilisateur identifié via un réseau de transmission de données, et des moyens (5) pour authentifier ledit utilisateur identifié et/ ou des messages vis-à-vis de ladite unité (4) en réponse à l'application d'un code d'authentification fonction dudit code variable. Les moyens de transmission comprennent un ensemble de récepteurs personnels (10) adressables sélectivement et dédiés chacun à un utilisateur habilité à accéder à ladite unité (4) et adaptés pour recevoir ledit code variable (Q) via ledit réseau (9) en réponse à l'identification de l'utilisateur correspondant, et le système comprend des moyens (7) de stockage de données pour l'adressage desdits récepteurs (10) en fonction desdites données d'identification appliquées auxdits moyens d'identification (5).



FR 2 769 446 - A1

La présente invention est relative à un système d'identification et d'authentification vis à vis d'au moins une unité électronique, pour le contrôle d'accès à une fonction et/ou l'authentification d'une personne et/ou d'un message.

Le développement de l'accès d'un public de plus en plus large à des systèmes ou réseaux informatiques ou similaires permettent d'accéder à des informations, d'échanger des données et/ou de réaliser des transactions telles que le télé-achat, la télévision à péage, la banque à domicile, le fac-similé confidentiel, etc..... nécessite la mise en place de mécanismes de sécurité performants.

Il est en particulier nécessaire, après qu'une personne se soit identifiée auprès d'un tel système informatique, par exemple au moyen d'un numéro d'identification personnel (PIN) connu en principe d'elle seule, de s'assurer par une procédure d'authentification que l'opération effectuée (demande d'accès, transmission de message, transaction en ligne, etc....) émane bien d'une personne autorisée.

Une procédure d'authentification de type connu repose sur la signature d'aléa. Après qu'un utilisateur se soit identifié auprès du système informatique, celui-ci lui adresse un nombre ou code aléatoire ou pseudo-aléatoire. Côté utilisateur, cet aléa est chiffré dans une unité d'authentification telle qu'une carte à puce, un dispositif électronique portable et autonome protégé physiquement contre les accès à ses circuits électroniques, un microordinateur personnel (PC), etc... A cet effet, cette unité est pourvue de circuits électroniques permettant d'effectuer un chiffrement de l'aléa au moyen d'un algorithme de chiffrement (DES, RSA, etc...) et d'une clé secrète ou personnelle. Le résultat de ce chiffrement est un mot de passe ou code d'authentification qui est appliqué par l'utilisateur au système informatique. Ce dernier effectue un calcul semblable sur l'aléa ou déchiffre le mot de passe : s'il y a cohérence entre le mot de passe généré par l'unité d'authentification et le résultat du calcul effectué par le système informatique, l'opération effectuée par l'utilisateur est authentifiée. Bien

entendu chaque fois qu'une procédure d'authentification est mise en œuvre, l'aléa généré par le système informatique est différent afin d'offrir une protection élevée contre les tentatives de cryptanalyse.

Un système informatique mettant en œuvre la procédure d'authentification du type précité fait appel à des unités d'authentification (carte à puce, dispositif électronique portable et autonome, PC, etc...) pourvues de moyens d'interface leur permettant de recevoir l'aléa ou code variable généré par le système informatique.

Dans les systèmes connus, il peut s'agir d'un lecteur de carte à puce, de moyens de lecture optique d'informations affichées sous forme codée sur un écran d'affichage, d'un modem, etc...

Ces systèmes ont notamment pour inconvénient qu'après qu'un utilisateur se soit identifié auprès du système informatique, celui-ci envoie l'aléa à l'utilisateur ou à l'unité d'authentification via l'interface de communication utilisée pour la procédure d'identification, de sorte qu'un tiers connaissant le numéro d'identification personnel (PIN) d'un utilisateur et en possession de son unité d'authentification peut s'authentifier frauduleusement auprès du système informatique.

L'invention vise à fournir un système d'authentification par signature d'aléa qui offre une sécurité accrue et une plus grande souplesse d'utilisation par rapport aux systèmes existants.

A cet effet, l'invention a pour objet un système d'authentification vis-à-vis d'au moins une unité électronique, comprenant :

- des moyens d'interface pour l'introduction de données d'identification et/ou d'authentification,

- des moyens d'identification d'utilisateurs en fonction de données d'identification introduites via lesdites moyens d'interface,

- des moyens pour générer un code variable en réponse à l'identification d'un utilisateur par lesdits moyens d'identification,

- des moyens pour transmettre ledit code variable audit utilisateur identifié via un réseau de transmission de données, et

- des moyens pour authentifier ledit utilisateur identifié et/ou des messages vis-à-vis de ladite unité en réponse à l'application d'un code d'authentification fonction dudit code variable,

caractérisé en ce que lesdits moyens de transmission comprennent un ensemble de récepteurs personnels adressables sélectivement et dédiés chacun à un utilisateur habilité à accéder à ladite unité et adaptés pour recevoir ledit code variable via ledit réseau en réponse à l'identification de l'utilisateur correspondant, et ledit système comprend des moyens de stockage de données pour l'adressage desdits récepteurs en fonction desdites données d'identification appliquées auxdits moyens d'identification.

Selon d'autres modalités remarquables de l'invention :

- le système comprend des unités d'authentification associées à chaque utilisateur et comportant des moyens pour générer ledit code d'authentification par chiffrage dudit code variable au moyen d'une clé secrète et d'un algorithme de chiffrement.

- lesdits moyens pour authentifier ledit utilisateur et/ou lesdits messages comprennent une unité de vérification pour contrôler ledit code d'authentification reçu de ladite unité d'authentification en fonction dudit code variable, de ladite clé secrète et d'un second algorithme.

- ledit réseau est un réseau de télécommunications.

- lesdits récepteurs sont des postes téléphoniques portables.

- lesdits récepteurs sont des messagers de poche.

- lesdits récepteurs comprennent un écran d'affichage dudit code variable .

- lesdites unités d'authentification sont intégrées chacune à l'un desdits téléphones portables.

D'autres caractéristiques et avantages de l'invention résulteront de la description qui va suivre, faite en se référant aux dessins annexés sur lesquels la figure unique est un schéma bloc d'un système d'authentification selon l'invention.

En se reportant à la figure unique, le système d'authentification selon l'invention comprend une unité d'authentification 1 pourvue d'une interface utilisateur telle qu'un clavier 2 et adaptée pour transmettre des données via une interface 3 à un système informatique 4. De préférence, la liaison entre l'unité d'authentification 1 et le système informatique 4 via l'interface 3 est bidirectionnelle de manière à permettre à la première de recevoir également des données du second.

Le système informatique 4 comprend une unité de vérification 5 connectée à un serveur 6 pourvue d'une base de données 7.

Le serveur 6 est connecté par une liaison 8 à un réseau de télécommunication 9 pourvu de récepteurs personnels 10 adressables sélectivement et comportant chacun une interface utilisateur telle qu'un écran 11.

L'unité d'authentification 1 peut revêtir différentes formes :

- il peut s'agir par exemple d'un dispositif électronique portable et autonome, c'est-à-dire pourvu de sa propre source d'alimentation électrique de ses circuits électroniques, lesquels comprennent un microcalculateur, des mémoires RAM et ROM, et des circuits d'interface avec le clavier 2 et éventuellement d'autre organes périphériques tels qu'un écran d'affichage 12. L'interface 3 peut être constituée par une liaison câblée avec un microordinateur personnel connecté au système informatique 4 par un modem ; l'interface 3 peut également être constituée par des phototransistors 13 aptes à lire optiquement des informations affichées sous formée codée sur l'écran d'affichage d'un terminal et par un clavier associé à ce terminal pour y introduire des données affichées sur l'écran 2 de l'unité 1 ; l'interface 3 peut également être constituée par une combinaison des moyens décrits ci-dessus ou par tout autre moyen connu des spécialistes de la technique permettant d'échanger des données entre l'unité 1 et le système informatique 4. Un tel dispositif électronique portable et autonome est décrit par exemple dans le document EP-A-0 552 822.

- il peut s'agir également d'une carte à puce associée à un lecteur permettant d'assurer l'alimentation électrique des circuit électroniques de la carte et l'échange de données entre la carte et un terminal connecté au système informatique 4.

- il peut s'agit encore d'un ordinateur personnel ou équivalent convenablement programmé connecté au système informatique 4, ou d'un terminal connecté à un ordinateur faisant partie ou connecté en réseau dans le système informatique.

Quelle que soit la forme revêtue par l'unité d'authentification 1, celle-ci est pourvue de circuits électroniques lui permettant, entre autres, de mémoriser des données telles qu'un numéro d'identification personnel (PIN), un algorithme de chiffrement C, une ou plusieurs clés secrètes K, etc... en vue de chiffrer un code variable ou aléa Q introduit via le clavier 2 et de générer un mot de passe ou code d'authentification A qui sera affiché sur l'écran 12.

Les récepteurs 10 sont constitués, par exemple, par des téléphones portables cellulaires ou des dispositifs de réception de message ou messagers de poche ("pager"). Ces récepteurs 10 ont la possibilité de recevoir des messages alphanumériques transmis par le réseau 9 et qui sont affichés sur l'écran 11.

Un utilisateur qui souhaite s'authentifier ou authentifier un message auprès du système informatique 4 doit être en possession d'un récepteur 10 qui lui est spécialement dédié. Il s'agit de préférence d'un téléphone cellulaire ou d'un messager de poche détenu par l'utilisateur à des fins de communication. Ainsi, à chaque utilisateur est associé un numéro d'appel qui est celui de son téléphone cellulaire ou de son messager de poche. Les numéros d'appel de l'ensemble des utilisateurs sont stockés dans la banque de données 7 en correspondance avec les numéros d'identification personnels (PIN) ou autres codes permettant à ces utilisateurs de s'identifier auprès du système informatique 4. De plus, de manière classique, l'utilisation du récepteur 10 peut être subordonnée à l'introduction dans celui-ci via un

clavier (non représenté) d'un code d'identification personnel, qui peut être ou non le même que le numéro d'identification personnel vis-à-vis du système 4.

En fonctionnement, un utilisateur qui souhaite accéder au système informatique 4 doit s'identifier auprès de son unité d'authentification 1 en introduisant son numéro d'identification personnel (PIN). Il doit également s'identifier auprès du système informatique 4, par exemple au moyen de ce PIN transmis par l'unité 1 via l'interface 3 ou introduit manuellement sur un clavier de l'interface 3. En variante, l'utilisateur peut s'identifier auprès du système informatique 4 au moyen d'un code secret ou non différent du PIN, par exemple un code affiché par ou inscrit sur l'unité 1.

Lorsque l'utilisateur a été identifié par le serveur 6 dans sa base de données 7, l'unité de vérification 5 génère un aléa Q et le serveur 6 transmet au réseau 9 cet aléa avec le numéro d'appel associé dans la base de données 7 au code d'identification de l'utilisateur qui a formulé la demande d'authentification.

Le central du réseau de télécommunication 9 adresse sélectivement l'aléa Q au récepteur 10 de l'utilisateur qui s'est identifié et cet aléa Q est affiché sur l'écran 11 du récepteur 10.

L'utilisateur lit l'aléa Q sur l'écran 11 et l'introduit dans son unité d'authentification 1 via le clavier 2. L'unité d'authentification calcule un mot de passe ou code d'authentification en chiffrant l'aléa Q au moyen de la clé K grâce à l'algorithme de chiffrement C.

Le mot de passe est transmis de l'unité 1 à l'unité de vérification 5 via l'interface 3. Parallèlement un calcul est effectué dans l'unité de vérification 5 en utilisant la même clé K, associée dans la base de données 7 au numéro ou code d'identification de l'utilisateur. Ce calcul peut consister par exemple à chiffrer également l'aléa Q par la clé K au moyen de l'algorithme A et à comparer le résultat de ce chiffrement avec le mot de passe reçu de l'unité d'authentification 1 : s'il y a concordance, l'utilisateur, ou un message transmis par celui-ci, sera authentifié par le système informatique 4. Le calcul effectué par l'unité de vérification 1 peut également consister à

effectuer certaines opérations sur le mot de passe reçu de l'unité 1 au moyen d'un algorithme B et de la clé K et à vérifier s'il y a cohérence entre le résultat obtenu et l'aléa Q.

Le système suivant l'invention permet ainsi de renforcer la sécurité de la procédure d'authentification par signature d'aléa grâce au fait que l'aléa est transmis, non pas de manière banalisée vers l'unité d'authentification d'où provient l'identification de l'utilisateur, mais sélectivement vers un récepteur dédié et personnel à cet utilisateur. La sécurité du système peut encore être renforcée en prévoyant que l'aléa ne sera affiché sur l'écran 11 du récepteur 10 qu'après introduction dans celui-ci, par l'utilisateur via un clavier, d'un code personnel différent ou non du PIN de l'unité 1.

Le système selon l'invention présente également l'avantage de ne faire de préférence appel qu'à des infrastructures de communication et/ou télécommunication existantes pour la mise en œuvre de la procédure d'authentification. Il permet en outre de mettre en œuvre cette procédure d'authentification dans l'hypothèse où l'interface 3 entre l'unité 1 et le système 4 ne permet pas de transmettre l'aléa Q du second à la première.

Le système d'authentification selon l'invention offre encore l'avantage d'assurer l'authentification du système informatique vis à vis de l'utilisateur lorsque le réseau de télécommunications 9 est un réseau public : en effet, pour transmettre l'aléa Q au récepteur approprié 10, le système informatique 4 doit se connecter au réseau 9 et par conséquent s'identifier vis à vis de lui. Pour renforcer encore la sécurité, une procédure d'authentification du système informatique 4 vis à vis du réseau 9 peut en outre être prévue lors de la demande de connexion. Le réseau 9 constitue ainsi un tiers dont la mémoire informatique du trafic permettra éventuellement de résoudre des conflits qui pourraient naître entre, par exemple, un fournisseur de produits ou de services et un utilisateur qui aurait passé en ligne une commande auprès de ce fournisseur.

Bien entendu de nombreuses modifications pourraient être apportées au mode de réalisation décrit sans sortir pour cela du cadre de l'invention.

C'est ainsi, par exemple, que l'aléa Q peut être transmis sous forme codé par le système 4 au récepteur 10, après quoi il est décodé dans l'unité 1.

Par ailleurs, l'unité d'authentification 1 et le récepteur 10 peuvent éventuellement être confondus dans l'hypothèse où les circuits électroniques du récepteur 10 sont agencés de manière appropriée pour effectuer les opérations dévolues à l'unité 1. Dans ce cas, l'affichage de l'aléa Q sur l'écran 11 n'est pas indispensable : à réception de l'aléa Q, le récepteur 10 effectue le calcul du mot de passe et affiche directement celui-ci sur l'écran 11. Cette solution renforce encore la sécurité en rendant plus difficile à des tiers l'accès à l'aléa Q, sous forme codée ou non.

REVENDICATIONS

1. Système d'identification et d'authentification vis-à-vis d'au moins une unité électronique, comprenant :

- des moyens d'interface pour l'introduction de données d'identification et/ou d'authentification,

- des moyens d'identification d'utilisateurs en fonction de données d'identification introduites via lesdites moyens d'interface,

- des moyens pour générer un code variable en réponse à l'identification d'un utilisateur par lesdits moyens d'identification,

- des moyens pour transmettre ledit code variable audit utilisateur identifié via un réseau de transmission de données, et

- des moyens pour authentifier ledit utilisateur identifié et/ou des messages vis-à-vis de ladite unité en réponse à l'application d'un code d'authentification fonction dudit code variable,

caractérisé en ce que lesdits moyens de transmission comprennent un ensemble de récepteurs personnels (10) adressables sélectivement et dédiés chacun à un utilisateur habilité à accéder à ladite unité (4) et adaptés pour recevoir ledit code variable (Q) via ledit réseau (9) en réponse à l'identification de l'utilisateur correspondant, et ledit système comprend des moyens (7) de stockage de données pour l'adressage desdits récepteurs (10) en fonction desdites données d'identification appliquées auxdits moyens d'identification (5).

2. Système selon la revendication 1, caractérisé en ce qu'il comprend des unités d'authentification (1) associées à chaque utilisateur et comportant des moyens pour générer ledit code d'authentification (A) par chiffrage dudit code variable (Q) au moyen d'une clé secrète (K) et d'un algorithme de chiffrement (C).

3. Système selon la revendication 2, caractérisé en ce que lesdits moyens pour authentifier ledit utilisateur et/ou lesdits messages comprennent une unité de vérification (5) pour contrôler ledit code d'authentification (A)

reçu de ladite unité d'authentification en fonction dudit code variable (Q), de ladite clé secrète (K) et d'un second algorithme.

4. Système selon l'une quelconque des revendications 1 à 3, caractérisé en ce que ledit réseau (9) est un réseau de télécommunications.

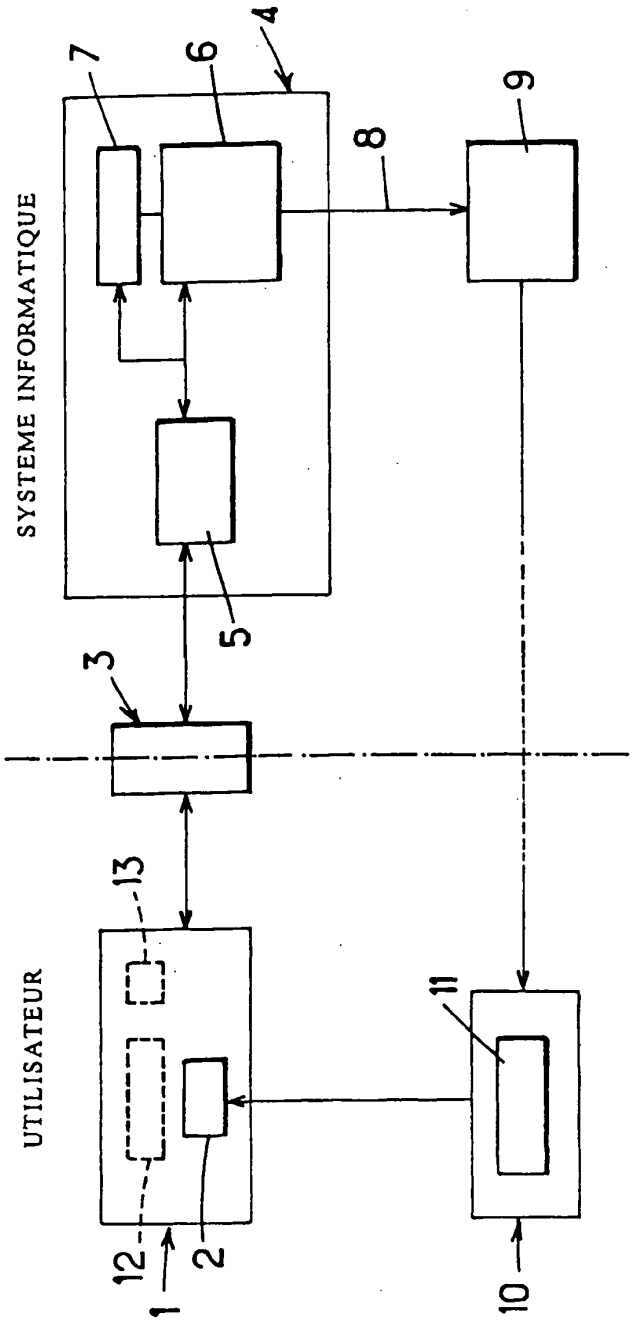
5. Système selon la revendication 4, caractérisé en ce que lesdits récepteurs (10) sont des postes téléphoniques portables.

6. Système selon la revendication 4, caractérisé en ce que lesdits récepteurs (10) sont des messagers de poche.

7. Système selon l'une quelconque des revendications 1 à 6, caractérisé en ce que lesdits récepteurs (10) comprennent un écran (11) d'affichage dudit code variable (Q).

8. Système selon les revendication 2 et 5, caractérisé en ce que lesdites unités d'authentification (1) sont intégrées chacune à l'un desdits téléphones portables (10).

1_1



REPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRELIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

2769446
N° d'enregistrement national

FA 550837
FR 9712277

DOCUMENTS CONSIDERES COMME PERTINENTS		Revendications concernées de la demande examinée
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	
X	WO 96 00485 A (ERICSSON TELEFON AB L M) 4 janvier 1996 * page 4, ligne 24 - page 15, ligne 21; revendications *	1-8
Y,D	EP 0 552 822 A (TELECASH) 28 juillet 1993 * abrégé; figures * * colonne 8, ligne 42 - colonne 11, ligne 54 *	1-8
Y	WO 97 31306 A (NOKIA MOBILE PHONES LTD ;SORMUNEN TONI (FI); KURKI TEEMU (FI)) 28 août 1997 * page 5, ligne 33 - page 9, ligne 11; figures *	1-8
A	WO 96 24913 A (NEXUS 1994 LTD) 15 août 1996 * abrégé; revendications; figures *	1,4-6
A	EP 0 565 279 A (AMERICAN TELEPHONE & TELEGRAPH) 13 octobre 1993	
A	US 5 130 519 A (BUSH GEORGE ET AL) 14 juillet 1992	

DOMAINES TECHNIQUES RECHERCHES (Int.CL.6)

G07F

1

Date d'achèvement de la recherche	Examinateur
10 août 1998	Meyl, D

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C13)